Email encryption using Tri-cryptosystem based on android

[1] Surendra Seervi; [2] Prem Parmar; [3] Niraj Viadya; [4] Hari Rajai
[4]*Assistant Professor*
[1-3]*B.E. Students*
Department of ComputeEngineering,
K.C. College of Engineering & Management studies Research
Kopri, Thane (E)-400 603, India

Abstract—*In the growing era of Digital Technology, a common question arise from digital users whether the digital Application is secure or not. Since the application is designed on a language the attacker always try to find new loop holes and has a result a new type of criminal activities take place. Even best encryption can be breached to corrupt the data, steal information, Cyber fraud, etc. This paper focuses on Email Security on Android Operating System by implementing the Tri-cryptosystem which is a combination of Symmetric cryptosystem, public key cryptosystem and hash function.*

Keywords– tri-cryptography, symmetric encryption, asymmetric encryption, hash function, secure email

I. INTRODUCTION

A most popular internet service is e-mail. Email is way to exchange text by using internet connection. Now almost internet services can be enjoyed by using mobile devices such as notebook, smart phone and tablet PC anywhere and anytime. Purposely, or not, the usage of e-mail to exchange information and collaborate, is not only limited to public information, but also confidential information, To certain parties which has a value of confidentiality so that it needs some security controls.

By using mobile devices with internet connection, e-mail services can be used widely by many people to exchange information and collaborate, both for individual, enterprise and government. One of the most popular Operating System is Android.

In order to prove safety of email sent from Android smart phone, encryption and decryption process have to be installed in an client side. All security systems use cryptographic because it suggest several algorithms and techniques practically unavailable to break because of their entanglement.

II. TRI-CRYPTOSYSTEM SYSTEM

Symmetric and asymmetric ciphers each have their own merits and demerits. Symmetric ciphers are faster than asymmetric ciphers, but require all parties to somehow share a secret key. But at the cost of speed asymmetric algorithms allow public key infrastructures and key exchange systems [4].

A Tri-cryptosystem is a protocol using multiple ciphers of different types together, each to its best merits. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the private key. Both the encrypted secret key and the encrypted message are then sent to the recipient.

The recipient decrypt the secret key first, using his/her own private key, and then uses that key to decrypt the message.

A. SYMMETRIC CRYPTOGRAPHY

An encryption system in which the sender and receiver uses a single, common key that is used to encrypt and decrypt the message. In contrast with public key cryptography, this utilizes two keys - a public key to encrypt messages and a private key to decrypt message. Symmetric-key systems are simpler and faster, but the main drawback is that the two parties somehow exchange the key in a secure way.

B.ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography is also known as public key cryptography, uses public and private keys for encryption and decryption of the data. The keys are simply large numbers that have been paired together but are not similar(asymmetric). One key in the pair can be shared with the parties; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the other key from the one used to encrypt the message is used for decryption[3].

C. Hash function

the process of transforming input message m into a fixed size string (called a hash value h) is called as hash function and it is denoted by H.here h is the output of hashing function applied on input message m.

h=H(m).hash function protect the integrity of the message .if attacker tries to modify the original message then the content of original message may changed it can be identified by applying hashing algorithm.

III EXISTING SYSTEM

In existing system by using mobile devices with internet connection, email services can be widely used by many people to exchange information and collaborate, both for individual, enterprise and government. One of the most popular Operating System is Android. In order to prove safety of email sent from Android smart phone, encryption and decryption process have to be installed in an client side. All security systems use cryptographic because it suggests several algorithms and techniques practically unavailable to break because of their entanglement

Limitation of existing system:

- More processing time
- Message digest length is more
- Less security

IV.PROPOSED SYSTEM

In this proposed design methodology, the new protocol design using Symmetric cipher (Ping Pong-128) and

public key cryptography (RSA) with hash function MD5. This kind of cryptography uses a single key for both encryption and decryption, and it is also called secret key cryptography. The key is a set of rules, and both the sender and the receiver must know the key in order to use the technique. The most commonly known secret key cryptography schemes are stream ciphers and block ciphers[1]. The stream ciphers generate a sequence of bits used as a key called a key stream, and the encryption is achieve by combining the key stream with the plaintext. This is usually done with the bitwise XOR operation. The key stream can be independent of the plaintext and cipher text, in which the stream cipher is synchronous, or it can depend on the data and its encryption, in which the stream cipher is self- synchronizing[2]. The public key cryptographic algorithms are more secure then symmetric algorithms. Because, it has two keys one for encryption and another one for decryption. In this tri-encryption technique we propose symmetric encryption for encryption and decryption and using public key cryptosystems for authentication A hash function offers a way of creating afixed-size blocks of data by using entry data with variable length and the exit data are known as message digest or one-way encryption. . The hash values solve the problem of the integrity of the messages.

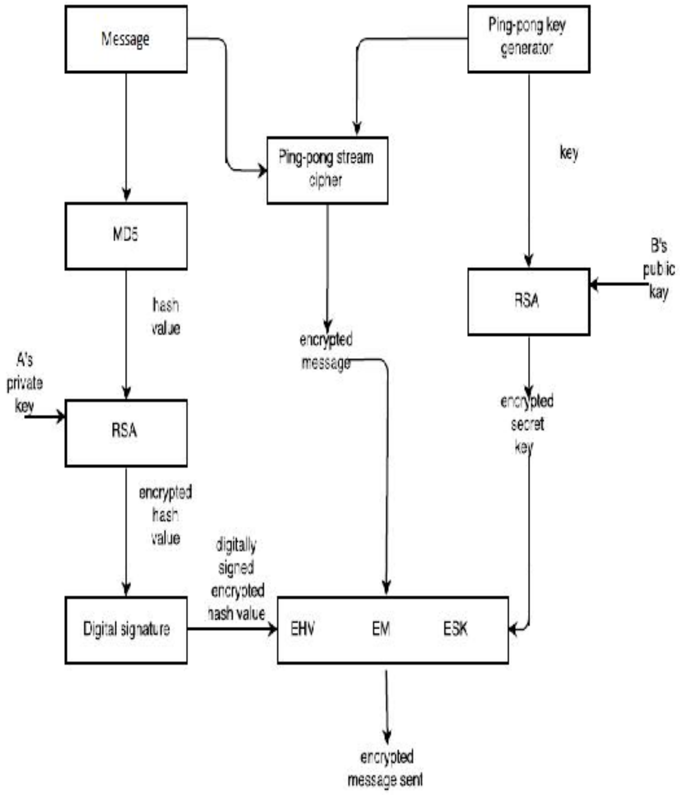

Fig: encryption process

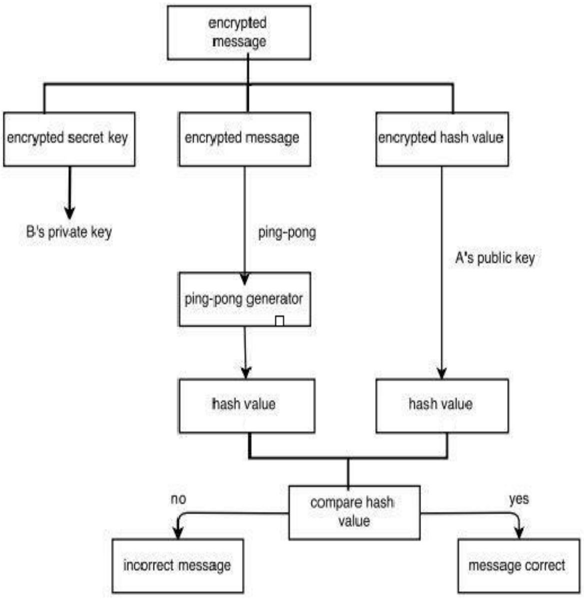

Fig: decryption process

For email encryption various algorithm is required:

4.1 Ping Pong

The advantage of a stream cipher is faster and much more efficient than block ciphers. PingPong-128 is a member of the Ping-Pong family key-stream generator which uses LFSR A (La) and LFSR B (Lb) of size 127 and 129 bits respectively and has a key size of 128 bits. These 128 bits of key and an initial vector of 128 bits are combined to fill up the 256 bits internal state. The Ping-Pong generator produces the output key stream by combining the LFSR sequences and the memory sequence [5] .

PingPong-128 uses two primitive polynomials, Pa(x) and Pb(x) which are given below

PA(X)=X127⊕ X109⊕ X91⊕ X84⊕ X73⊕ X6⊕ X66⊕ X63⊕ X56⊕ X55⊕ X52⊕ X48⊕ X45⊕ X42⊕ X41⊕ X37⊕ X34⊕ X30⊕ X27⊕ X23⊕ X21⊕ X20⊕ X19⊕ X16⊕ X13⊕ X12⊕ X7⊕ X6⊕ X2⊕ X1⊕ 1

Pb(x)=x129⊕ x125⊕ x121⊕ x117⊕ x113⊕ x109⊕ x105⊕ x101⊕ x97⊕ x93⊕ x89⊕ x85⊕ x81⊕ x77⊕ x73⊕ x69⊕x65⊕ x61⊕ x57⊕ x49⊕ x45⊕ x41⊕ x37⊕ x33⊕ x29⊕ x25⊕ x21⊕ x17⊕ x13⊕ x9⊕ x5⊕ 1

The feedback connection of LFSR A (La) and LFSR B (Lb) is determined by the primitive polynomials, Pa(x) and Pb(x) respectively. Since primitive polynomial is used for the feedback connection, both of the LFSRs generate maximal length sequence. LFSR A (La) has a period of 2^127-1 and LFSR B (Lb) has a period of 2^129 - 1.

4.2RSA

RSA is a block cipher which convert plain text into cipher text at sender side and vice versa at receiver side .The security of RSA is considered to be factoring. RSA computation occurs with integers modulo n = a * b, for two random secret primes a, b. To encrypt a message m, public key use a public key exponent e. so cipher text c = me (mod n) computes the multiplicative reverse of d = e-1 (mod (a-1)*(b-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n)[4]. The problem for the attacker is that computing the reverse d of e is assumed to be no easier than factorizing n. The key size should not be less than 1024 bits for a reasonable level of security.

Digital signature employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through not secure channel: Properly implemented, a digital signature gives the receiver proof or feedback to believe the message was sent by the claimed sender. To create RSA signature keys, generate an RSA key pair containing a modulus *N* that is the product of two large primes, along with e and d such that ed=1 (mod φ (n)) of*N* and *e*, and the signer's secret key contains *d*.

To sign a message *m*, the signer computes $\sigma \equiv m^d$ (mod *N*). To verify, the receiver check that $\sigma^e \equiv m$ (mod *N*).

As noted earlier, this basic scheme is not very secure. To prevent attacks, one can first apply a cryptographic hash function to the message *m* and then apply the RSA algorithm described above to the result[6].

4.3.MD5

MD5 is a one way hash function, means it takes a message of arbitrary length and converts it into a fixed string of digits which is called as message digest.

When using a one way hash function, one can compare the message digest that is decrypted with a public key against the calculated message digest to verify that the message has not been tampered .

Conclusion

Most of us use smart phone, tablet and computer all day long without realizing it. So, we need to realize the encryption for application of smart phone/Android OS. Tri-cryptosystem makes use of two different cryptographic algorithm. Which removes the drawback of use of any single cryptographic algorithm and provide double security to secret data? It removes key distribution problem. It's strengths are respectively defined as speed and security. Therefore, we are suggesting the design of tri-cryptographic for secure email based on Android OS.

Acknowledgment

This work is a part of graduation project done by students of computer engineering. We thank everyone who supported and motivated us. And special thanks to our guide Mr. hari Rajai.

[1] William Stallings (2003), Cryptography and Network Security-Principles and Practices, 3rd Edition, Pearson Education Asia

[2] Menezes AJ, Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. Florida: CRC PressInc. 1996.

[3] Ramaraj E, Karthikeyan S, Hemalatha M. A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA). International Journal of The Computer, the Internet and Management. 2009; 17(1):78-86

[4] Prof.PatrickMcDaniel,NetworkandSecurityResearch CenterDepartmentofComputerScienceandEngineeringPennsylvaniaState University, UniversityPark PA – "Public-Key Cryptography andAttacks on RSA", 2010

[5] Prof.HoonJae Lee, Kevin Chen, 2007 International Conference on Convergence Information Technology "PingPong-128, A New Stream Cipher for Ubiquitous Application"

[6] https://en.wikipedia.org/wiki/Digital_signature.